U.S. Department of Transportation
Federal Aviation Administration

Advisory Circular

Subject: COMPLIANCE CRITERIA FOR 14 CFR §33.28, AIRCRAFT ENGINES, ELECTRICAL AND ELECTRONIC ENGINE CONTROL SYSTEMS.

Date:
Initiated By:
Cosimo Bosco, ANE-110

AC No: 33.28-1
Change:

1. **PURPOSE.** This Advisory Circular (AC) provides guidance and acceptable methods, but not the only methods, that may be used to demonstrate compliance with §33.28 of Title 14 of the Code of Federal Regulations (14 CFR). Like all AC material, this AC is not, in itself, mandatory and does not constitute a regulation. While these guidelines are not mandatory, they are derived from extensive Federal Aviation Administration (FAA) and industry experience in determining compliance with the pertinent regulations.

2. **RELATED REGULATIONS AND READING MATERIAL.**

a. Related Regulations. Sections 21.16, 33.4, 33.5, 33.17, 33.19, 33.49, 33.75, 33.91(a), Appendix A of part 33, 23.901, 23.903, 23.1309, 25.901, 25.903, 25.939, 25.1181, 25.1309, 27.901, 27.903, 27.1309, 29.901, 29.903, 29.1309

b. Advisory Circulars, Notices and Policy Letters/Memoranda.

(1) AC 20-115B, RTCA, Inc. Document RTCA/DO-178B, dated January 11, 1993 (AMJ 20-115B) (RTCA Document RTCA/DO-178B/EUROCAE ED-12B).

(2) AC 20-136, Protection of Aircraft Electrical/Electronic Systems Against the Indirect Effects of Lightning, dated 3 May 1990 (SAE-AE4L 87-3 REV B dated October 1989).

(3) AC 20-53A, Protection of Aircraft Fuel Systems Against Fuel Vapor Ignition Due to Lightning, dated April 22, 1991.

(4) High Energy Radiated Electromagnetic Fields (HERF), Interim Policy Guidelines on Certification Issues, dated 5 December 1989, issued by AIR-100.

(5) Federal Aviation Administration (FAA) Notice N8110.71, Guidance For The Certification of Aircraft Operating in High Intensity Radiated Field (HIRF) Environments, issued April 2, 1998.

(6) AC 21-16D (RTCA DO-160D/EUROCAE ED-14D) Environmental Conditions and Test Procedures for Airborne Equipment, dated July 21, 1998.

(7) Policy Memorandum, FAA Engine and Propeller Directorate Policy Regarding Time Limited Dispatch (TLD) Of Engines Fitted With Full Authority Digital Engine Control (FADEC) Systems, dated October 28, 1993.

(8) AC 33-2B Aircraft Engine Type Certification Handbook, dated June 30, 1993.

c. Industry Documents

(1) RTCA Document No. DO-160D (EUROCAE ED14D), Environmental Conditions and Test Procedures for Airborne Equipment, dated July 29, 1997.

(2) RTCA Document No. DO-178B (EUROCAE ED12D), Software Considerations in Airborne Systems and Equipment Certification, dated December 1, 1992.

(3) SAE ARP 5107, Guidelines for Time-Limited-Dispatch for Electronic Engine Control Systems, issued June 1997.

(4) SAE ARP 4754, Certification Considerations for Highly-Integrated or Complex Aircraft Systems, issued November 1996.

(5) SAE ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems, issued December 1996.

(6) SAE ARP 926A/B Fault/Failure Analysis Procedure.

(7) SAE ARP 1834/A Fault/Failure Analysis for Digital Systems.

d. Military Specifications.

(1) MIL-STD-461D, Requirements for the Control of Electromagnetic Interference Emissions and Susceptibility, dated January 11, 1993.

(2) MIL-STD-462D, Measurement of Electromagnetic Interference Characteristics, Test Standard For**,** dated February 5, 1996.

(3) MIL-STD-810E, Environmental Test Methods and Engineering Guidelines, dated July 31, 1995.

(4) MIL-HDBK-217F, Reliability Prediction of Electronic Equipment, dated February 28, 1995

(5) MIL-HDBK-179A, Microcircuit Acquisition Handbook, dated July 20, 1995.

3. **APPLICABILITY**. This document applies to electrical and electronic engine control (EEC) systems used on aircraft engines certificated under part 33 of Title 14 of the Code of Federal Regulations (part 33) and for use in aircraft certificated under parts 23, 25, 27, and 29. This document also applies to any electrical or electronic systems that control an engine function, for example

overspeed or temperature limiting systems. Lastly, in some cases, controls for functions not normally covered under part 33 or required for engine control are integrated into the EEC, for example, propeller controls regulated under part 35. In these cases, this document also applies to those functions integrated into the EEC system, but only to the extent that those functions affect part 33 requirements.

4. **DEFINITIONS**.

a. Alternate Control or Operating Mode(s). For the purposes of this AC, an alternate control or operating mode is one in which the operating characteristics or capabilities of the engine control are sufficiently different from the "normal mode" that the operating characteristics or capabilities of the aircraft, crew workload, or what constitutes appropriate crew procedures may be significantly impacted or changed.

b. Commercial and Industrial Grade Electronic Parts. Commercial (consumer quality parts) and industrial grade parts have typical operating ranges of 0 degrees to +70 degrees Celsius and -40 degrees to +85 degrees Celsius, respectively. Commercial and industrial grade parts are typically defined in these temperature ranges in vendor parts catalogs.

c. Electronic Engine Control (EEC) System. This is the generic family of electrical/electronic engine control systems that includes FADEC controls, supervisory controls, and derivatives of these.

d. Full Authority Digital Engine Control (FADEC). This is a control system in which the primary functions are provided electronically and the electronic unit has full-range authority over the engine power or thrust. FADEC systems have been certificated that employ two identical channels to provide full-operational capability after failure of one channel, or a single channel with a simplified electronic or hydromechanical back-up providing an alternate operating mode. The "FADEC system" includes all the control elements identified in the instruction manual, including sensors, wiring and mechanical, pneumatic or hydromechanical components and other limiter or protection devices. If the control requires data from aircraft computers to operate, this data is considered a part of the EEC or FADEC system, and the interface requirements for this data should be specified in the engine instruction manual. Mechanical components, such as the fuel pump, that are not interfacing with the EEC system are generally not included in the definition of FADEC system components.

e. Fault or Failure. This is an occurrence that affects the operation of a component, part, or element such that it can no longer function as intended and includes both loss of function as well as a malfunction. Errors that may cause failures are not considered as failures.

f. Fault or Failure Condition. This is a condition having an effect on the airplane or its occupants, either direct or consequential, that is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events.

g. Fault or Failure Detection. This term refers to the discovery of a fault or failure condition and either announcement of that condition to the flight crew by instrumentation or storage of the detection of that condition, or its results, in a fault memory for later retrieval through a built-in test capability of that control.

h. Fault or Failure Accommodation. This term refers to the capability of the control system or crew to mitigate, either wholly or in-part, the failure condition.

i. Full-up System or Configuration. For the purposes of the system safety assessment (SSA) analyses described in this AC, the "full-up system" is one that has no faults or failures present, detected or undetected, that affect the control of engine power or thrust, engine protection systems, indication of critical engine operating parameters or other safety features of the control. A "full-up" system would be one in which everything is operative.

j. Loss of Thrust Control (LOTC). This term refers to the loss of capability to modulate and maintain thrust or power between flight idle and 90 percent of maximum rated power or thrust at all operating conditions (see paragraph 4.c.(4)(a) of this AC). One Engine Inoperative (OEI) or Automatic Take-off Thrust Control System (ATTCS) ratings and implementations are exempted from an LOTC analysis, because the portion of time spent at these ratings is relatively small, and they are covered by aircraft level analyses.

k. Per Hour. When the term "per hour" or "per flight hour" is used in this AC, the definition is "per engine flight hour."

l. Range of Control. This term refers to modulation of the engine from idle to 100 percent max rated thrust or power and includes any red line or higher rotor speed protection controls and any engine temperature, torque, and pressure limits set and implemented by the control.

m. Take-off Envelope. This term refers to the operation of the aircraft at or below 1500 feet above ground level (AGL) during take-off or landing approach. In cases in which distant obstacle clearance is involved, the take-off envelope may be to a higher altitude than 1500 ft. AGL. For rotorcraft the take-off envelope is considered to be 1000 feet AGL for Category A rotorcraft, and within the height-velocity envelope for all others.

n. Uncovered Fault. A fault or failure for which either no detection mechanism exists or, if detected, no accommodation exists.

o. Unsafe Condition. For purposes of this AC an unsafe condition is one that prevents continued safe flight and landing of the aircraft and must be extremely improbable, that is the probability per engine flight hour should be less than 10E-09 events/hour. Failures of the EEC system that may be classified as unsafe under certain conditions are discussed in this AC.

5. **BACKGROUND.**

a. This advisory circular provides guidance material for methods of complying with §33.28, Electrical and Electronic Engine Control Systems. Section 33.28 was added to part 33, Airworthiness Standards: Aircraft Engines, as Amendment 15 (58 FR 29095, 5/18/93) and became effective on August 16, 1993.

b. An accompanying advisory circular was not issued at the time because there was an FAA initiative to reduce the amount of advisory material by providing a rule with sufficient information to minimize the need for additional advisory material.

c. Initially EEC technology was primarily applied to engines designed for large transport aircraft applications. The certification practice and implementation of §33.28 was oriented toward these applications. When the use of EEC technology was limited to a small group of manufacturers, the information and guidance provided in the rule itself was adequate. With the proliferation of EEC controls, however, it has become evident in several recent engine certification programs that there is a need for additional advisory material.

d. In addition, industry representatives from the engine community that design engines for applications other than large transport aircraft certificated under part 25 have questioned the criteria used to determine equivalence to the typical hydromechanical system. One of the basic criterion for FAA acceptance for the replacement of hydromechanical technology with electronic technology for engine controls is that the new technology must have an equivalent level of integrity and reliability as the technology being replaced. Because the data used to establish the criteria for equivalent reliability of a

typical hydromechanical system was based on part 25 certification experience, other industry representatives have presented a valid argument that the equivalence criteria to a hydromechanical system should be based on data for hydromechanical control systems used in their respective part 23, 27, and 29 certifications.

SIGNATURE

CONTENTS

APPENDIX

1. **SECTION 33.28 - GENERAL.** One of the objectives for the engine manufacturer in an engine certification program is to show that the certificated engine will be "installable" in a particular aircraft or aircraft type. If the aircraft application is unknown at the time of engine certification, the engine manufacturer should make reasonable installation and operational assumptions for the anticipated aircraft application to achieve this objective. In order to facilitate achieving this objective, the engine manufacturer should provide a document that describes the EEC system and its operation to both the office with responsibility for the engine certification program and to the office with responsibility for the aircraft certification program. The aircraft certification office will determine if the EEC system complies with the applicable aircraft certification regulations (§XX.901, §XX.903 and §XX.1309 of parts 23, 25, 27, and 29). Providing the EEC documentation to the aircraft certification office is particularly important when the system is novel or unique and differs from previously certificated systems. The engine certificating office will also coordinate with the appropriate FAA engine controls specialist(s) in this regard. If these reviews indicate that the engine may not be installable in the intended aircraft type, then the engine certificating office will inform the applicant and the appropriate aircraft certification office of any potential certification issues. This coordination with the aircraft certification office is only considered necessary for the initial aircraft application of the engine. If no aircraft is identified as the anticipated installation for the engine, a review may be conducted with the applicable standards staff. Any installation limitations or operational issues will be noted in the Installation or Operational Manuals and the Type Certification Data Sheet (TCDS).

Lastly, applicants should be aware that the aircraft certification office may require flight testing to fully evaluate engine performance and operability characteristics for all operating modes.

2. **SECTION 33.28(a).**

a. Rule Text. Section 33.28(a) provides that each EEC must, **"Have the control system description, the percent of available power or thrust controlled in both normal operation and failure conditions, and the range of control of other controlled functions, specified in the instruction manual required by §33.5 for the engine."**

b. Intent of Rule. Section 33.28(a) ensures that the engine installer is provided with sufficient information regarding the EEC system to have a clear understanding of the control system in the normal and any alternate control or operating modes. Any differences in operation in other than the normal mode should be clearly defined. Also, any subtle interface requirements, such as power interrupt tolerance of the EEC, should be clearly defined. The percent of available power or thrust in both normal operation and any alternate modes should be specified. Range of control of other controlled functions should also be specified.

c. Background. The following guidance provides a method, but not the only method, of compliance with §33.28(a).

(1) Control System Description. The applicant should include a brief control system description in the instruction manual and may incorporate a more detailed system description document by reference. Consideration should also be given to other functions integrated into the EEC system. If functions other than those directly associated with the control of the engine are integrated into the EEC system, such as thrust reverser control, propeller control or automatic starting, descriptions of these functions should also be included in the instruction manual. Even if the FADEC control is integrated wholly or in part within an aircraft avionics system, the engine manufacturer should provide an engine control system description to the extent of the applicant's responsibility related to part 33 engine certification requirements and should include the relationships of the engine control system to the aircraft systems. Engine control systems that are embedded in aircraft avionics may require special conditions as prescribed under §21.16.

(2) Interface Description. The instruction manual should include installation interface descriptions, limitations, and requirements of the engine control system. For example, the EEC power requirements and quality, including interrupt limitations, should be clearly defined for the engine installer. Another example is that the impedance and buffering limitations for the signals provided by the EEC system for display and instrumentation, or signals used by the EEC, such as air data information, should be specified to ensure that the EEC system is adequately isolated and unaffected by other systems using these signals.

(3) Operational Description.

(a) The instruction manual should contain a description of the control system operating characteristics in both the normal and alternate control or operating modes. Restrictions in the flight envelope or unusual operating characteristics in these alternate modes should be clearly defined. Any abnormal control characteristics that could have an impact on crew procedures, training, workload, or any other aspects of aircraft performance or operating characteristics should be identified for evaluation during aircraft certification.

(b) If dispatch of the control system with faults has been approved by a time-limited-dispatch (TLD) analysis or other analyses, the instruction manual, or other appropriate documentation, should include the time limitations pertaining to this type of operation. If no TLD or other appropriate analysis or documentation is submitted to substantiate the acceptability of dispatching the engine control with faults present or portions of the control inoperative, the control may be restricted to "full-up" dispatch only. Any abnormal control characteristics that could have an impact on crew procedures, training, workload, or any other aspects of aircraft performance or operating characteristics should be identified for evaluation during aircraft certification.

(c) Faults will occur which leave the control in a non-dispatchable configuration. The instruction manual should indicate how the EEC system will announce that condition to the flight crew. It should also describe how the control system provides "output information" of such a

condition. Faults that leave the control in a condition that cannot meet part 33 requirements are generally considered non-dispatchable.

(d) For fault conditions that are approved as dispatchable by the engine certificating office, the instruction manual should describe how information concerning these fault conditions is available from the control or elsewhere, and the "time limits" approved for such operations. Approval by the engine certification office that a particular fault condition is dispatchable does not guarantee that the aircraft certification office or the operator's certificate management office will approve that same condition as dispatchable for the aircraft or that operator.

(4) Substantiation Data. The instruction manual should include data from analyses conducted to comply with §§33.28(b) and (c) (discussed in paragraphs 3 and 4 of this AC), data from the environmental testing conducted to comply with §33.28(d) (discussed in paragraph 5 of this AC), and data from the software level determinations conducted to comply with §33.28(e) (discussed in paragraph 6 of this AC). This data will assist the installer in safely installing the engine. The following specific data should be included:

(a) The applicant should have available and provide, as required, data for all operating modes to demonstrate that the control meets its design intent.

(b) The applicant should have available and provide, as required, data to show that a progressive means of increasing power or thrust with throttle or load demand is provided for all control modes.

(c) Data for the following:

1. The software level (for each function, if necessary).

2. The estimated failure rates for:

(i) Engine shut-down in-flight due to engine control causes.

(ii) Loss of engine or propeller control or significant change in power or thrust.

(iii) Failures to the back-up system.

(iv) Transmission of faulty parameters that affect cockpit located engine displays, or other safety critical functions.

(v) Loss of any critical safeguards, such as overspeed or valves needed for fire protection.

(vi) Loss of any aircraft-supplied data or power required to assure proper engine operation.

(vii) Other safety significant failure conditions, such as the probability of an uncontrolled overspeed and the other control system associated events as determined from the system safety analysis (SSA). A control system event is one that the control system causes or is involved in preventing.

(d) The types and levels of environmental exposure for which the EEC system has been successfully qualified should be stated, for example, vibration, temperature, HIRF, and lightning. For new applications of a previously certified control system, substantiation of the environmental capability of the EEC system by similarity analyses, as well as tests, may be acceptable. The certification approach to be pursued should be indicated in the certification plan. For HIRF, lightning and electromagnetic interference (EMI) qualification tests, the interfacing aircraft cables used for the tests should be described.

(5) Fault Accommodation Logic Data.

(a) The applicant should have available and provide, as required, a tabulation of the fault accommodation logic for the critical parameters used by the control.

(b) The applicant should have available and provide, as required, a tabulation of the "default" or "fail-safe" states of all EEC system outputs and the rationale for their selection.

3. **SECTION 33.28(b).**

a. Rule Text. Section 33.28(b) provides that each EEC system, **"Be designed and constructed so that any failure of aircraft-supplied power or data will not result in an unacceptable change in power or thrust, or prevent continued safe operation of the engine."**

b. Intent of Rule. Section 33.28(b) ensures that the engine and control continue to function in a safe and reliable manner in the event of the failure of aircraft-supplied power or data, or both, while providing sufficient flexibility to accommodate the increasing engine and aircraft integration that accrues from the use of electronic control technology.

c. Background. The following guidance provides a method, but not the only method, of compliance with §33.28(b).

(1) Unacceptable Change in Power or Thrust. The office with responsibility for the engine certification program will decide for each program, on a case by case basis, what constitutes an "Unacceptable change in power or thrust." Further discussion on loss of power or thrust can be found in paragraph 4 of this AC. Although complete or partial loss or change

of thrust or power in a single engine is not necessarily an unsafe condition for multi-engined aircraft, the engine certification office will evaluate both partial and complete loss of power or thrust. This evaluation includes the frequency, duration and percentage of power or thrust change that results from the failure of aircraft-supplied data or power. This evaluation also considers location in the flight regime at the time of the event. The applicant should provide analytical or test data that can be used in this evaluation. This data may include worst case plots of percentage power or thrust change over the declared operating envelope for failure of aircraft-supplied data or power.

(2) Failure of Aircraft-Supplied Data. "Aircraft-supplied data," in this context, includes all analog, discrete and digital data provided by the aircraft systems to the EEC. The applicant should define in the instruction manual the effect of the failure of aircraft-supplied data on the engine's output power or thrust characteristic throughout the flight envelope. The above data should be provided for all allowable engine control and aircraft dispatch configurations in which the loss of aircraft power or data in that dispatch configuration would result in a different engine control system response. Examples of system configurations that have been found to be acceptable under §33.28(b) include:

(a) Dual sources of aircraft-supplied data with local engine sensors provided as "voters" and alternate data sources. Sensors that act as "voters" provide a method for the EEC system to determine if one of the primary data sources is providing erroneous data, and to then, if so, eliminate that erroneous source from consideration. In the event of a failure in the aircraft-

supplied data, the engine sensors act as the primary source of sensed data through the fault accommodation logic. In the event of the loss of this engine-sensed data, the system uses modeled or synthesized parameters.

(b) In some cases, a system may use synthesized engine parameters as voters. The applicant should provide data that gives the worst case percentage change of power or thrust over the declared operating envelope when inaccuracies of the synthesizing process are considered as well as the environmental effects on the sensors used in the synthesis.

(c) It may be acceptable to use a third source of aircraft-supplied data as the voter in lieu of engine sensors. In this case, when aircraft data is used exclusively, the following items should be addressed, if applicable, in the SSA or other appropriate documents:

1. Software in the data path to the EEC should be at a level consistent with that defined for the EEC. The data path may include other aircraft equipment, such as aircraft air data computers (ADC), thrust management computers, or other avionics equipment. If the software levels in the computers generating data used by the EEC, or in the computers in the data path to the EEC, are not at a consistent level with EEC software, then the use of that data in the EEC should be limited so as not to cause LOTC events or inappropriate engine operating events.

2. The applicant should state in the instruction manual that the aircraft manufacturer must ensure that changes to aircraft equipment, including software, in the data path to the engine do not affect the integrity of the data provided to the engine as defined by the instruction manual.

3. If dispatchability of the aircraft without a third source required by the system as the voter is anticipated, analysis that demonstrates the acceptability of this dispatch configuration must be provided for the Minimum Maintenance Equipment List (MMEL) or for the TLD documents, as applicable.

4. Since aircraft-supplied data has an effect on EEC system operation, the effects of faulty and corrupted aircraft data on the EEC system should be supplied in the engine instruction manual. It is assumed in the three ADC configuration that the EEC system would be significantly affected by erroneous or faulty air data information and that the engine could experience a significant thrust or power change during such a condition. If this is the case, the applicant should indicate in the instruction manual that air data information, and any other aircraft information that could have a significant impact on engine thrust or power, is considered critical to EEC system operation, and therefore, the installer should ensure that those sensors and equipment involved in delivering that information to the EECs are capable of operating in the "severe" HIRF and lightning environments, as defined in the certification basis for the aircraft, without impact to their proper and continued operation.

5. The reliability level for the aircraft-supplied data that was used as part of the SSA and LOTC analysis, as discussed in paragraph 4 of this AC, will be stated as an "assumed value" in the instruction manual.

(d) Fault accommodation for the complete loss of ADC inputs or other aircraft-supplied data, even though this loss may be extremely improbable, should be provided. In this case, sufficient testing or analysis, or both, should be conducted on the fault accommodated control mode to establish that the engine operating characteristics comply with all operability requirements of part 33.

(3) Common Mode Faults. In the exchange of data with the aircraft, consideration should be given to elimination of unacceptable common mode faults affecting the operation of more than one engine or propeller. Limits for unacceptable common mode faults that affect power or thrust are described in the discussion of §33.28(c) (paragraphs 4.c.(4)(c), 4.c.(4)(d), and 4.c.(4)(e) of this AC). Common faults that affect engine protection limit systems or could hazard the aircraft would generally be unacceptable. The logic included in the control system to accommodate common faults should be demonstrated. Any precautions needed to address common effects may be taken either through the aircraft system architecture or by logic internal to the engine control system. This may be demonstrated as part of the software integration testing during the EEC software verification or EEC system validation test program.
In particular, the following cases should be considered:

(a) Erroneous data received from the aircraft by the engine or propeller control system, if the data source is common to more than one engine or propeller, for example air data sources, autothrottle systems, and synchronizing controls.

(b) Control system operating faults propagating via data links between engine or propeller, for example, maintenance recording, common bus, cross-talk, auto-feathering, and automatic power reserve system.

(c) Loss or interruption of aircraft data or electrical power used by the engine control, when that loss or interruption is caused by the failure of another engine.

(d) Exchange of data between engines to implement control functions, for example, load sharing and synchrophasing, should be shown to incorporate authority limits in order to prevent unacceptable common mode loss of power or thrust.

(4) System Integration. The trend toward system integration may lead to EEC systems that utilize resources distributed within the aircraft in addition to the aircraft-supplied data described above. In these cases, the office responsible for certifying the engine will look to the engine manufacturer to specify the requirements for the EEC system, as described in the instruction manual, and to substantiate the adequacy of those requirements. These requirements are defined in the instruction manual to ensure that the engine certification basis is maintained. These may include, but are not limited to, the following:

(a) Software levels should be compatible with the software levels used in the EEC system hazard assessment.

(b) Software partitioning, if applicable, should comply with DO-178B guidelines.

(c) Lightning, HIRF, and EMI testing should demonstrate that the EEC system is not adversely affected when exposed to these environments.

(d) Reliability requirements for control system elements located in the aircraft that form any part of EEC system type design should be defined.

(e) The effects of faults on the continued environmental qualification of the EEC system should be addressed. This is important if multiple engines may share a common interface or if these faults could remain undetected long enough that they are anticipated to be present simultaneously on multiple engines.

(5) Fault Accommodation Logic. The applicant should perform an SSA to determine the adequacy of the EEC fault accommodation logic. Functionality of the fault accommodation logic should be demonstrated. This demonstration may be conducted as part of the system integration testing.

(6) Control System Elements Mounted in the Aircraft. There may be elements of the control system that are mounted in the aircraft that are powered by and dedicated to the EEC, such as a throttle position transducer. In these instances, the element is considered to be an integral component of the EEC system and faults should be accommodated as such, rather than as aircraft-supplied data. The method used for addressing single and dual failures of these signals should be documented and the fault accommodation for these signals demonstrated. The demonstration may be completed as part of the software integration testing during the EEC software verification testing.

(7) Failure of Aircraft-Supplied Power. The applicant should demonstrate that the EEC control system can continue to function normally with the failure or interruption of aircraft-supplied power at any point within the declared engine operating envelope. Some engine control functions that have traditionally relied exclusively upon aircraft electrical power are excepted from compliance with this requirement because their good service history indicates they provide an equivalent level of safety for compliance with this rule. The applicant should define in the instruction manual the impact of the failure of aircraft-supplied electrical power on the output power or thrust characteristics of the engine throughout the flight envelope. The following are examples of these functions:

(a) Non-critical functions;

(b) Engine start;

(c) Ignition;

(d) Thrust reverser;

(e) Anti-icing; and

(f) Fuel shut-off.

(8) Aircraft-Supplied Power as Backup Power. Aircraft-supplied power may be used as a backup source of power to the dedicated engine-mounted alternator in the event of an alternator failure. If the control is not required to have a dedicated power source and uses aircraft power as its normal power supply, such as a system with a full hydromechanical back-up, and the transition from the electronic to the hydromechanical control is acceptable, then this does not apply.

4. **SECTION 33.28(c).**

a. Rule Text. Section 33.28(c) provides that each EEC must, **"Be designed and constructed so that no single failure or malfunction, or probable combination of failures of electrical or electronic components of the control system, results in an unsafe condition;"**

b. Intent of Rule. Section 33.28(c) ensures that the complete engine control system, including the electrical and electronic parts, provides a system that is considered equivalent in safety and reliability to engine control systems that are based on more conventional hydromechanical technology. Current regulations based on hydromechanical technology rely on testing and mechanical inspection intervals to ensure control system reliability and airworthy operation. Electronic technology does not lend itself to mechanical inspection. Therefore, to ensure safe operation after an electrical or electronic component failure, redundancy techniques and self-monitoring have been required in EEC systems to achieve equivalent control system integrity. Previous EEC systems have used the design approach of showing that the EEC system is essentially single fault tolerant with respect to electrical or electronic failures when establishing safety and reliability equivalence to conventional hydromechanical systems. The word "essentially" is used because it may not be practical to accommodate all failures. In the TLD analysis a two (2) percent default value is assigned in some cases to these uncovered faults for a full dual channel redundant system.

c. Background. The following guidance provides a method, but not the only method, of compliance with §33.28(c).

(1) Replacement of Hydromechanical Technology. The objective in accepting the transition from hydromechanical control (HMC) technology to electronic control technology is to maintain at least an equivalent level of system reliability and safety. A review of several

hydromechanical control system designs shows that the mean time between control system failures that have a significant effect on engine operation is approximately 100,000 hours.

(2) Engine Controls for Part 25 Aircraft Applications. For engines used in large transport aircraft, the criteria used in early certification programs to establish that an EEC had an equivalent level of safety and reliability to an HMC was that an EEC system should not cause more than one LOTC event per 100,000 engine operating hours. An LOTC event is discussed in paragraph 4.c.(4)(a)1. of this AC. Redundancy techniques may be provided in the system by electronic, HMC, or other means. In general, engines designed for installation on transport category airplanes utilize a fully capable dual channel FADEC or a single channel FADEC with a fully capable HMC.

(3) Engine Controls for Aircraft Applications Other Than Large Transport Aircraft. For applications other than transport category airplanes, such as general aviation aircraft certified under part 23 and both normal and transport category rotorcraft, certified under parts 27 and 29, the LOTC rate of one (1) event per 100,000 engine hours is also acceptable. However, criteria other than the 100,000 hour LOTC rate may be appropriate, depending on the reliability demonstrated by the previous control systems used on those engines, provided that in-service experience has proven that reliability of those previous systems to be satisfactory. In this case, an acceptable system LOTC rate, that is a rate equivalent to the hydromechanical systems being replaced, of more than one (1) event per 100,000 engine hours may be acceptable. These new systems will still be expected to be "essentially" single fault tolerant with respect to electrical or

electronic failures. In these systems, transfer to an alternate mode(s) should not be considered an LOTC event in the analysis, provided the alternate mode(s) satisfies the applicable LOTC guidelines provided in this AC. An acceptable system reliability rate may be achieved by using a functionally dissimilar hydromechanical or electronic system with reduced capability.

(a) The acceptability of these alternate systems should be assessed on the basis of the following criteria:

1. Compliance of the alternate system with the requirements of part 33. Any exceptions should be identified and assessed with respect to proposed operational usage. In no case should backup or alternate functions result in an unsafe condition.

2. The failure rate from the primary control mode to the alternate system.

3. The LOTC rate of the control system.

4. Pilot workload and performance during transition to or during operation in an alternate control mode. This issue may need evaluation at the aircraft level. The engine manufacturer should coordinate with the aircraft manufacturer, if known, and the aircraft certification office to determine whether the alternate operating modes comply with the applicable aircraft certification standards. These issues have been significant for some programs.

(b) Factors to be considered in the design and evaluation of any alternate operating mode(s) should include, but are not limited to, the following:

1. Automatic protection from surge or lean limit blow-out.

2. Acceleration and deceleration times.

3. Altitude relight capability.

4. Dormant failures of the alternate operating mode and documentation of any automatic or manual checks to ensure the availability of the mode.

5. Dispatchability, if any alternate modes are intended to be dispatchable.

(4) System Safety Analysis (SSA).

(a) The applicant should complete and have available for review and acceptance an SSA for the EEC control system, addressing all declared dispatchable control configurations. Data used in the SSA should be substantiated. The SSA should include, but not necessarily be limited to, the following events caused by engine control system malfunctions:

1. Failures affecting thrust:

(i) Loss of the ability to modulate power or thrust between the selected idle and 90 percent of maximum rated power or thrust at all operating conditions. This failure mode is considered an LOTC event. Minor deviations in idle thrust caused by faults affecting that control function may be allowable. A fault that increases idle thrust too much may be a concern in the aircraft approach configuration, because it affects the aircraft's ability to maintain the desired approach angle or glide-slope, and a fault that decreases idle thrust too much may effect cowl anti-icing and go-around thrust capabilities. Therefore, while faults that result in not setting the proper idle thrust do pose a concern, small deviations from the correct, selected idle thrust due to small sensor errors, for example, should be acceptable. These conditions should be examined in the engine failure modes and effects analysis (FMEA) and the aircraft SSA.

(ii) Engine shutdown, which is a subset of all LOTC events.

(iii) Unwanted changes in magnitude or direction of power or thrust.

(iv) Instability in the control of a critical function.

2. Transmission of faulty parameters, including engine indications such as oil pressure, rotor speed, inter-turbine or exhaust gas temperature, the engine's thrust parameter if not rotor speed, engine power or torque, etc.

3. Unwanted action of a critical control function, such as deployment of reversers.

4. Degradation in the capability of executing a critical function, such as failure to auto feather.

5. Inability of the engine to meet part 33 requirements, such as loss of engine protection features as outlined in paragraph 4.c.(6) of this AC.

(b) When applicable, failure rates should also be provided for loss of ancillary control functions and engine indications that directly or indirectly lead to engine shutdown, such as the following:

1. Stability augmentation.

2. Oil, engine case, or component cooling.

(c) The SSA should consider the extent of power or thrust changes resulting from undetected faults:

1. When operating in the take-off envelope, an uncovered fault in the control system or of an aircraft signal used by the engine control system that results in a thrust or power

change of less than three (3) percent on the engine has generally been considered acceptable. However, this does not detract from the applicant's obligation to ensure that the full-up system is capable of providing the declared minimum rated thrust or power during take-off. Such faults should be random in nature and should be detectable and correctable during routine inspections, overhauls or power-checks.

2. Undetected faults in an aircraft signal that result in a thrust or power change greater than three (3) percent should be declared in the approved engine instruction manual. This data should describe the magnitude of the thrust or power change and the flight condition associated with the condition. Larger than three (3) percent undetected thrust or power changes have generally been considered acceptable when operating outside the take-off envelope. In previous aircraft applications, these "outside the take-off envelope" thrust or power changes have been limited to less than approximately 15 percent and have been allowed in conditions involving high altitude or high speed, or both.

(d) During take-off, detected faults in aircraft signals used by the engine control that result in a thrust or power change of up to 10 percent may be acceptable if their frequencies of occurrence are relatively low. In previous applications, frequencies of less than 10^{-5} events per flight hour have been accepted.

(e) Single or multiple electrical or electronic failures, as well as hydromechanical system failures, that cause a greater than 10 percent change in power or thrust should be

included in the control system's LOTC analysis. In this analysis, a safety factor or margin should be used for the frequencies of occurrences for "single" electrical or electronic failures that result in a greater than 10 percent thrust or power change when a field service data base is not available to support the data used in the analysis. A factor of two (2) is recommended. If a single electrical or electronic failure can result in an engine configuration that does not comply with part 33, this should be included in the SSA. The frequencies of occurrence of single electrical or electronic failures that cause thrust or power changes less than 10 percent, but greater than three (3) percent, or result in the engine not meeting part 33 requirements, should be reviewed with the office handling the engine certification for acceptance.

(f) The SSA should provide allowance for uncovered faults and their effects on the control system. This acknowledges the potential presence of faults that can affect thrust or power and may not be recognized in the FMEA and SSA and, therefore, for which no fault accommodation is provided. It is generally assumed that uncovered faults, which can have a greater than 10 percent influence on engine thrust or power, lead to LOTC events. Therefore, the fault rate for these uncovered faults should be included in the LOTC analysis, and the rate used should be substantiated.

(g) If the SSA assumes that a particular crew action is used to mitigate the impact of a fault condition, that assumed crew action should be clearly detailed in the instruction manual. The acceptability of this crew action may need to be validated at the aircraft level during aircraft certification. If the applicant requires a particular crew action to avoid an unsafe condition, the

applicant should specify the display requirements associated with the failure condition in the instruction manual.

(h) The SSA should consider potential faults in aircraft wiring associated with the engine control. The effect of a grounding or over-voltage condition on any EEC system wiring caused by opens or shorts in that wiring to other aircraft wiring or structure shall be contained in the engine instruction manual. Special note should be made for any dispatch configuration in which the open, short, or over-voltage condition would cause an LOTC event. In addition, opens and shorts to ground of the engine harness wiring should be shown by test or analysis, or both, to result in a safe engine response.

(i) The applicant should have available for review an FMEA. The FMEA can be based on a piece part failure analysis or a functional analysis. Since FMEAs are usually completed from a complete type design configuration, performing an FMEA by completing a piece part failure analysis on redundant electrical or electronic components is not particularly useful, because the effect or result for most of these failures is "no effect." For the purposes of understanding the failure modes of a redundant EEC system, the intent of the propulsion control system FMEA should be to understand the system with regard to single failures. Hence, the analysis should be focused on those single elements of the control that cause an impact on the control system and, therefore, engine operation. Of particular interest are those single electrical or electronic and mechanical or hydromechanical failures that affect the operation of the control system. These may be undetected or uncovered faults as well as detected faults. Some of the

failures that should be considered are failures that cause the control system to change engine power or thrust, not respond to throttle inputs, lose the capability of shutting off fuel, cause the engine to overspeed, cause loss of a protective function, cause the control to "fail fixed" or change modes, or cause the control to fail to a state that requires pilot intervention. Mechanical or hydromechanical failures that cause the engine to possibly increase in power or thrust and disable or reduce the capability of a protective function, like the overspeed protective function, should be investigated and reviewed to determine whether the design should be altered or changed to avoid such a situation. The analysis is intended to determine the criticality of single failures.

(5) Control Mode Transitions. Systems that use alternate control modes as a backup system, including supervisory control systems, should incorporate automatic control features to transfer to the alternate mode when detected electrical or electronic failures occur that are otherwise not accommodated in the normal mode. In some applications a "fail fixed" fuel flow followed by a manually activated switch to the alternate mode has been accepted. In these situations, provisions for announcing the "fail fixed" condition to the flight crew by cockpit instrumentation should be made. The alternate mode may be implemented using hydromechanical, electrical or electronic means, or any combination of these. The power or thrust change associated with an automatic transfer to the alternate mode should be declared in the approved engine instruction manual. Generally, designs involving automatic transfers have been limited to thrust changes less than approximately 10 percent. Thrust changes larger than 10 percent have been accepted when resulting from a crew selected transfer. Acceptable

transition between all control modes should be demonstrated to the greatest extent possible for engine certification. Development flight testing is highly desirable, if available. If pilot action is required in the fault detection and transfer of control, the faults involved in such a situation should be declared in the engine instruction manual, and the condition(s) should be evaluated during aircraft certification. For transfers that occur automatically, consideration should be given to the following:

(a) The frequency of occurrence of transfers to any alternate control mode. Computed frequencies of transfer to any alternate control modes should be supported with data from endurance or reliability testing, in-service experience on similar equipment, or other acceptable data.

(b) Faults that would result in transfer to any alternate mode and the capability for detection of these faults.

(c) Self-test coverage and diagnostics. Sufficient self-test coverage and diagnostics should be provided to allow detection of error conditions critical to system performance.

(d) Any time delays in the transfer of control should be declared in the engine instruction manual. In some cases, it may not be possible for the engine certification engineer to determine that the mode transition provides a safe and acceptable system in accordance with part 33 based solely on analytical or simulation data. Therefore, it may be advantageous to the

applicant to propose a brief flight test program to support the data. In any case, such control transition delays may or may not be acceptable for aircraft certification, depending on the installation. Therefore, the engine manufacturer should coordinate with the aircraft manufacturer, if known, and the aircraft certification office to evaluate this configuration early in the program. Also, any control mode transition should be fully evaluated during aircraft certification.

(e) Availability of the alternate mode. If the alternate mode is not exercised during normal mode operation, an inspection interval or procedure for exercising the alternate mode should be specified to ensure that it remains functional and available. Any inspection interval or procedure may result in an operational limitation and requires the approval of the engine certification office.

(f) Provisions for signal(s) to indicate a mode transition.

(6) Overspeed Protection System Requirements. This applies to engine designs requiring an overspeed protection control function. Two categories of overspeed malfunction should be considered; those caused by shaft separation or loss of load, and those caused by control or fuel system failures. Overspeed malfunctions caused by shaft separation or loss of load may be too rapid for the overspeed protection system to react in a timely manner. Therefore, unless the control system is intended to provide such protection, this case does not need to be considered. For shaft failure cases, the engine design should have some alternate methods of protection

against rotor overspeed in order to comply with §33.75, such as "blade-shedding" or a "mash-and-clash" turbine design. In cases in which the engine design incorporates blade-shedding to protect the rotor from an overspeed above structural limits, a control system overspeed protection system may not be needed, because the blade-shedding approach is intended to work on any overspeed condition. For those engine designs using a "mash–and-clash" method of overspeed protection, an EEC overspeed protection system may be needed if the "mash–and-clash" design of the turbine provides protection only when the turbine shaft is free to move axially. If a control system overspeed protection function is necessary, the overspeed protection system should be evaluated with regard to functionality and reliability as part of the engine control system.

(a) For overspeed protection systems, the following provides one method, but not the only method, of compliance with both §§33.28 and 33.75:

1. The combined engine and overspeed protection system should be at least two faults removed from a potential rotor burst event, when one of the faults induces the overspeed. In this respect, a potential rotor overspeed burst should only be possible as a result of a first fault inducing an overspeed and an independent fault preventing the overspeed protection system from operating.

2. The analysis should show that the probability per engine flight hour of an uncontrolled overspeed condition from any cause in combination with failures of the overspeed protection system is less than one event per billion hours (E10-9).

3. The failure rate of the overspeed protection system, itself, should be on the order of one event per ten thousand hours (E10-4) per hour.

4. The probability of an inadvertent trip of the overspeed protection system should be commensurate with the fault consequences. The frequency of inadvertent trips of the overprotection protection system that cause a greater than ten percent thrust or power change should be included in the LOTC analysis.

5. Overspeed protection is a necessary function for dispatch and is required by §§33.28(c) and 33.75. Therefore, when the overspeed protection function is part of the control system and its implementation involves the use of electrical or electronic components, a self-test of the overspeed protection system to ensure that the system is functional prior to each flight should be implemented. It has been acceptable to verify functionality of the overspeed protection system at engine shutdown of the previous flight.

6. When multiple paths can invoke the overspeed protection system, a test of a different path should be performed each engine cycle such that a complete test of the overspeed system is achieved in a minimum number of engine cycles. If a path(s) is found to be

inoperative, the failure rate of the remaining path(s) should be less than 10^{-4} failures per hour, and combinations of failure leading to an uncontrolled overspeed event should still be extremely improbable. In no case should the control system be knowingly dispatched with the overspeed protection system failure rate greater than 10^{-4} failures per hour or known to be inoperative.

7. The applicant may provide data that demonstrates that the mechanical part of the overspeed protection system, such as the fuel shut-off mechanism, can operate without failures between stated periods, and the applicant may propose establishing a periodic inspection and test interval for the shut-off mechanism in lieu of testing shut-off mechanism operation as part of the self-test conducted for each flight. When this approach is used, the self-test conducted for each flight may be limited to the electrical and electronic components of the overspeed protection system.

8. Use of shared resources between the control system and the overspeed protection system should be evaluated. An analysis should show that the probability of faults of shared resources that could cause or contribute to an overspeed event as well as inhibit the overspeed protection function is extremely improbable, that is less than one event per billion engine flight hours (10E-09). Single failures should not cause such a condition. The intent is that the overspeed protection system should be independent from the normal control.

9. When the overspeed control function is implemented via mechanical or hydromechanical means only, such as a fly-ball governor system, a periodic inspection and test interval for compliance with the requirement for "continued system availability" is acceptable. The periodic inspection and test interval should be based on test or in-service data that demonstrates that the system operates without failure between intervals.

(b) The overspeed malfunctions utilized in the failure analysis should be addressed when complying with §33.27.

(7) Guidance for Use of Commercial or Industrial Grade Electronic Parts. When commercial or industrial grade electronic components are specified in the engine type design, the applicant should verify the commercial or industrial grade vendor's database upon which the failure rate of the component is based, and the applicant should have plans or procedures in place to assure that the basis for the declared vendor failure rate is maintained throughout the entire procurement and manufacturing cycle. Commercial and industrial grade electronic components are not defined, identified, or controlled by military specifications. The applicant should have available and provide the following data for review, as required:

(a) For each commercial and industrial grade electrical component specified in the design, the applicant should have reliability data that substantiates the failure rate for each component that is used in the EEC reliability analysis and in the SSA.

(b) The applicant should have procurement, quality assurance, and process control plans in place for the vendor-supplied commercial and industrial grade parts that can be used to assure that the parts will continue to be provided at the reliability level specified in the approved engine type design.

(c) Because commercial and industrial grade parts may not all be manufactured to the same accepted industry standard, such as military component standards, it may be necessary to provide unique databases for similar components procured from different vendors.

(d) If the declared installation temperature environment for the EEC is greater than that of the electronic components specified in the engine type design, the applicant should substantiate that the proposed extended range of the specified components is suitable for the application. Additionally, if commercial or industrial parts are used in an environment beyond their specified rating, and cooling provisions are required, the cooling provisions should be specified. Failure modes of the cooling provisions that cause these limits to be exceeded should be considered in determining the probability of failure when installed in the aircraft.

(8) Consideration of Local Events. When designing an electronic control system to meet the requirements of §33.28, the engine manufacturer should provide a control system with at least an equivalent level of safety and reliability as has been achieved by engines or propellers equipped with HMC systems. Such HMC systems have been shown to perform safely and reliably in the face of what are termed "local events." In some cases, the EEC system provides

functions not previously provided by HMC systems, or is implemented differently so that an equivalence comparison to the HMC system is not practical. In these cases the acceptability of the effect of local events should be based on the effect on aircraft safe flight and landing. Examples of "local events" include: engine overheating conditions or fires, electrical problems, hydraulic and lubricating fluid leaks, and mechanical disruptions.

(a) Whatever the local event, the behavior of the EEC system should not cause a hazard to the aircraft that could jeopardize continued safe flight and landing. This will require consideration of effects such as the control of the thrust reverser deployment, an overspeed of the engine, and transients effects or inadvertent propeller pitch change under any flight condition.

(b) When demonstrating that there is no hazard to the aircraft from local events that could jeopardize continued safe flight and landing, the applicant should show that any other function that is necessary to provide protection will be available at the time of the local event and will not be rendered inoperative by the same local event, such as destruction of wires, ducts, power supplies, etc. This includes proposed designs in which the engine manufacturer assumes the aircraft, or aircraft components, provides necessary protection. This assumption should be documented in the engine failure modes effects and criticality analysis (FMECA).

(c) An overheat condition exists when the temperature to which the EEC is exposed is greater than the maximum safe design operating temperature declared by the engine manufacturer. The electronic portions of the control should not cause a hazardous condition

when the EEC is exposed to a continuous overheat or over-temperature condition, such as may occur within a nacelle when a duct bursts or leaks. Specific design features or analysis methods may be used to show compliance with respect to the prevention of hazardous effects. When this is not possible due to the variability or the complexity of the failure sequence, then acceptable testing may be required. Computer simulation techniques similar to those discussed for fire testing in paragraph 4.c.(8)(d) of this AC have also been acceptable. The compliance criterion for overheat requires that when the EEC system is exposed to an overheat condition, the system should not cause the engine to behave in an unsafe manner and should allow a safe engine shut down.

(d) Section 33.28 requires that exposure of the electrical and electronic parts of the EEC system to fire will not result in an unsafe condition. The EEC system must comply with fire test requirements when the system is located in a fire zone. Fire zones are defined in appropriate aircraft certification standards. Fire requirements for the electronic parts of the EEC system are not covered precisely in the regulations with regard to the length of time they are required to function when exposed to fire. Therefore, a compliance criteria has been developed for EEC systems that requires that the control system maintain the ability to safely shut down the engine when exposed to fire. In addition, the system must not take an unwanted action that could become hazardous to the aircraft during the exposure to the fire. Therefore, when exposed to fire the EEC system should allow a safe engine shut down without an unwanted action occurring during the exposure.

1. The fuel handling parts of the EEC system, including the fuel shut-off valve (SOV), should comply with the requirements of §33.17, which requires these parts to be fire resistant. The engine design must minimize the probability of the occurrence and spread of fire. Therefore, consideration should be given to those parts of the EEC system that control airflow that could fail in a direction to contribute to the fire when the system is exposed to fire.

2. In addition, §33.75 requires that fire cannot cause the engine to lose the capability to shut down. For system designs that depend on electric power to actuate the SOV, it may be necessary to use high temperature wire or other protective means to ensure that the capability to shut down the engine is retained when exposed to fire.

3. Computer simulations of exposure of the EEC to fire may be used in lieu of fire tests on production hardware as demonstration of compliance with fire resistance requirements. Approved computer simulations should be validated by analysis or test, or both, including all assumptions upon which construction of the computer simulation is based.

4. Hardware emulations for use in fire tests may also be acceptable. Approved hardware emulations should be validated by analysis or test, or both.

5. The engine manufacturer should note that as part of aircraft certification for transport aircraft the Transport Airplane Directorate (TAD) has required actual fire tests be conducted on all elements in systems in which there is the potential for fire causing a

catastrophic failure, such as elements that could cause a catastrophic reverser deployment or an uncontained rotor burst.

(e) The applicant should demonstrate by analysis or test that when any EEC system component input or output electrical connection is open circuited or shorted to ground, the system behaves in a safe and predictable manner. In addition, it should be shown that any EEC system component connector that becomes disconnected while the engine is operating does not jeopardize the continued safe flight and landing.

(f) The applicant should demonstrate by analysis or test that hydraulic or lubricating leaks impinging on the EEC control system do not result in a hazard to the aircraft that could jeopardize the continued safe flight and landing.

(g) The applicant should demonstrate by test or analysis, or both, that mechanical disruptions that could sever connections or impact and damage EEC system components do not result in a hazard to the aircraft that could jeopardize continued safe flight and landing. It is recognized that evaluation of this design feature is installation dependent in many cases, and that the evaluation of the considerations in the design for mechanical disruptions may have to be considered on a case by case basis.

(9) EECs For Reciprocating Engines.

Reserved.

5. **SECTION 33.28(d).**

a. Rule Text. Section 33.28(d) provides that each EEC must, **"Have environmental limits, including transients caused by lightning strikes, specified in the instruction manual."**

b. Intent of Rule. Section 33.28(d) ensures that the engine and control system meet acceptable environmental operating conditions. The instruction manual should clearly define EEC system operational limitations, for the benefit of the engine installer, and provide assurance that the EEC system is functional in a reasonably designed aircraft environment.

c. Background. The following guidance provides a method, but not the only method, of compliance with §33.28(d).

(1) General Test Requirements. Section 33.28(d) requires that the EEC system have environmental limits specified in the engine instruction manual, including those associated with lightning and High Intensity Radiated Fields (HIRF). Environmental tests conducted on an individual system component basis in accordance with test procedures defined in RTCA Document DO-160D (see AC 21.16D), or equivalent, have been acceptable, except for temperature variation, HIRF and lightning tests.

(a) A minimum of 10 temperature cycles should be performed for temperature variation tests.

(b) For the HIRF, lightning, and electromagnetic interference (EMI) system tests, adaptation and combinations of the test procedures in RTCA Document DO-160D should be used. The test procedures contained in RTCA Document DO-160D are directed toward tests of individual pieces of equipment rather than systems, such as EEC controls.

(c) EMI tests conducted in accordance with MIL-STD-461/462 have been accepted as providing procedures and test levels equivalent to those in RTCA Document DO-160D. When the two test procedures differ for a particular test case, the more rigorous test procedure should be used unless use of the alternate test can be justified. HIRF and lightning tests should be conducted using the procedures described in paragraphs 5.c.(2), 5.c.(3), and 5.c.(4) of this AC.

(d) Environmental tests in accordance with MIL-STD-810E may be accepted in lieu of RTCA Document DO-160D tests when the MIL-STD-810E tests are equal to or more rigorous than those defined in RTCA Document DO-160D.

(2) System Test Configuration Considerations. HIRF, lightning, and EMI tests have been conducted as system tests by EEC manufacturers or engine manufacturers on closed loop laboratory setups. The closed loop setup is usually provided with hydraulic pressure to move

actuators to close the inner actuating loops. A simplified engine simulation may be used to close the outer engine loop.

(a) Open Loop Laboratory Tests. In some cases, open loop laboratory setups with EEC test software have been accepted. If the applicant elects to conduct open loop setups the following factors should be considered:

1. The EEC test software should be developed and implemented by guidelines defined for software levels of at least Level 2 or Level C, in RTCA Document DO-178A and RTCA Document DO-178B, respectively. In some cases, the application code is modified to include the required test code features.

2. The system test setup should be instrumented to monitor both the output drive signals and the input signals.

3. Anomalies observed on inputs or outputs should be duplicated on the engine simulation to determine whether the resulting power or thrust perturbations comply with the pass/fail criteria.

(b) Pass/Fail Criteria. The tests should be conducted with the EEC system controlling the engine at the most sensitive operating point, as selected by the applicant. This may be a different operating point for the three different tests. The system should be exposed to the

HIRF, lightning, and EMI environmental threats while operating at the selected condition. The pass criteria for HIRF and lightning is that there be "no effect" on the operation or operational characteristics of the system. "No effect" is defined as less than ± 2 percent of power or thrust change from the normal control governing capability for a period of less than one second. For other EMI testing, the limits selected from the appropriate section of RTCA/DO-160D have been used. The following results are considered to be test failures:

1. Transfers to alternate channels, backup HMC systems, or reversionary modes.

2. Component damage.

3. Significant fault codes recorded in the fault memory.

4. False fault announcements to the crew that could cause unnecessary or inappropriate crew action.

5. Erroneous operation of overspeed or reverser circuits.

(3) HIRF Test Requirements. For HIRF testing, systems have been accepted for engine certification based on the AIR-100 December 5, 1989, interim HIRF policy letter and supplements that address critical systems. Notice N8110.67, "Guidance for the Certification of Aircraft Operating in High Intensity Radiated Fields (HIRF) Environments," superseded the

interim HIRF policy letter. Due to the one year limitation of policy notices, N8110.67 was cancelled and the HIRF notice reissued as N8110.71 in April 1998. N8110.71 includes minor modifications and has a cancellation date of April 2, 1999. In the interim policy letter and the two notices, it is stated that using 100 volts per meter average from 10 KHZ to 18 GHZ was an acceptable level for conducting HIRF bench tests for systems that perform critical functions. For rotorcraft applications, the HIRF bench test level should be 200 volts per meter average from 10 KHZ to 18 GHZ.

(a) The Engine and Propeller Directorate has used 200 volts per meter average over the entire frequency range from 10 KHZ to 18 KHZ as the standard for testing EEC systems.

(b) At a minimum, the modulations specified in RTCA Document DO-160D, Section 20 for categories W or Y should be used. Additional modulations based on the EEC operating frequencies or control loop bandwidth should be used for the system HIRF tests.

(c) In many cases, additional pulse modulation tests in the microwave range are specified by the aircraft manufacturers. These additional tests are generally at field levels in excess of 1000 volts per meter. Experience to date has shown that EECs that pass 200 volts per meter average will also pass tests at the higher pulse modulated field levels at the higher frequencies. However, it should not be assumed that the system is hardened to these levels without completing the high level pulse tests. Test procedures generally follow the guidelines of Section 20 of RTCA Document DO-160D.

(4) Lightning Test Requirements. Lightning tests follow the guidelines of AC 20-136 and Section 22 of RTCA Document DO-160D. Multiple Stroke (MS) and Multiple Burst (MB) tests are conducted on the system connected on the test bench as described in paragraph 5.c.(2) of this AC.

(a) EEC MS Lightning Tests. Low level lightning test(s) should be conducted to establish the engine cable shield current levels. Low level tests have been used to establish the wave forms and current levels coupled on to the cables for the MS tests. The shield current level for large engines has been on the order of 1000 to 2000 amperes. For smaller engines, shield current levels have been higher. These levels are typically determined by low current level lightning tests on the engine without the full benefit of nacelle attenuation and, therefore, should be conservative. Although the shield current level is not required to be used in an MS lightning test, the applicant should demonstrate that the level is a realistic level for the category of engine and its application.

(b) EEC MB Lightning Tests. Past MB tests have been conducted using the chattering relay test defined in Section 19.3.4.1 of RTCA Document DO-160D. However, the chattering relay test has been superseded by MB tests using Waveform 3 or Component H defined in AC 20-136.

(c) EEC Pin Injection Tests (PIT). PITs are normally conducted on the EEC. PIT levels are selected as appropriate from the tables of Section 22 of RTCA Document DO-160D. PITs are conducted on other system components as required.

1. PITs should be used to verify that equipment does not exhibit permanent upset or damage when subject to the pin-injected transient waveforms. During these tests, the transient waveforms are applied directly to the designated pins on the equipment connector, normally between each pin and the equipment chassis ground, as described in RTCA Document DO-160, Section 22. This method is used to assess the dielectric withstand voltage or damage tolerance of the equipment interface circuit. For equipment electrical interface circuits that are electrically isolated from the equipment chassis or grounds, a dielectric withstand or high-potential (hi-pot) test that meets or exceeds the peak transient waveform voltage amplitude is acceptable in place of the PIT.

2. Equipment interface circuits with low impedance with respect to the equipment chassis should be subjected to the PIT. For pin injection purposes, low impedance should be considered less than 100 ohms at any frequency below 10 KHZ. Shunt filters and transient suppression devices such as Tranzorbs(tm) normally produce low impedance to chassis to provide transient protection and should be subjected to the PITs at the selected waveform levels.

(d) Aircraft and Engine Certification Lightning Tests. Lightning tests conducted on an EEC system may be adequate to cover aircraft certification, as well as engine certification, provided the aircraft-engine interface cables and current levels are adequately represented in the test. This applies to engine-mounted EECs. The test levels should be at a level compatible with the installation. The applicant and the engine certification office should mutually agree on the test level in the test plan. In order to account for the aircraft contribution to the test levels, it is desirable in some cases to coordinate with the aircraft certification office in order to use a mutually acceptable test level for the category of aircraft involved.

1. The engine manufacturer should note that each aircraft manufacturer installing an engine must determine the levels to which the installed engine and EEC system will be exposed for the particular aircraft and demonstrate that these levels are equal to or less than the levels that were used for engine certification testing. If the aircraft manufacturer cannot show that this is the case, then EEC system lightning tests may be needed to show compliance with aircraft certification standards.

(5) Maintenance Requirements. Section 33.4 and Appendix A to part 33 require that the engine manufacturer prepare Instructions for Continued Airworthiness (ICA) for all engine parts. As part of the ICA a maintenance plan must be provided. Therefore, as part of the environmental protection system that is part of the engine type design and used to protect the EEC system from HIRF and lightning, a maintenance plan must be provided to ensure the continued airworthiness of the installed systems.

(a) Notice 8110.71 provides some guidance that can be used to meet the ICA requirement. Maintenance requirements may include periodic inspections or tests for required structural shielding, wire shields, connectors, and equipment protection components. The applicant must provide the engineering validation and substantiation of these maintenance requirements.

(6) Environmental Testing. All components of the EEC system, including all electronics units, sensors, harnesses, hydromechanical elements, and any other relevant elements or units, are required to be tested to establish that they will operate properly in their declared environment. When applicable, tests defined in RTCA Document DO-160D have been accepted. Environmental test plans should be approved by the engine certification office prior to commencing the tests.

(a) Although environmental test limits are not specified, environmental tests should be representative of the environments that are expected to be encountered in the engine installation. Special attention should be given to any condition that could affect more than one engine or propeller control system, such as a faulty operation during hot day ambient conditions. The environment to which the component is qualified should be entered into the instruction manual and is considered to be an installation limitation for the installer.

(b) The applicant should prepare an environmental test plan that is summarized in an environmental test matrix that defines the method to be used to qualify the component for each of the environments. The environments and test procedures defined in RTCA Document DO-160D have been acceptable to the FAA for electrical and electronic components. Generally, only the anticipated types of environments to which the components are expected to be exposed need to be tested. For other environments the matrix can be noted as "not applicable." The components may be qualified by test, similarity, analysis, or any combination of these.

(c) For fuel handling, hydraulic, and pneumatic components, such as the Fuel Metering Unit (FMU) and actuators, the applicant should provide the proposed test plan for approval before commencing the tests of these components. These components may be qualified by test, similarity, analysis or any combination of these. In some cases, the testing required for the engine block tests under §§33.49 or 33.87 may be adequate to qualify these components. Otherwise, additional tests are required under §§33.28(d) and 33.91(a).

(7) Time Limited Dispatch (TLD) Environmental Tests. Although TLD is not a requirement for certification, HIRF and lightning tests for TLD are usually conducted together with tests conducted for certification. In order to gain approval for the use of TLD, applicants are expected to demonstrate that dispatchable EEC configurations continue to meet environmental requirements of the certification basis. SAE Document ARP 5107 also contains applicable TLD information. For HIRF and lightning, applicants have usually determined that

the single channel dispatch configuration is the worst case dispatch configuration and have conducted HIRF and lightning tests with one channel inoperative to demonstrate compliance. For other environments, the applicants have complied by analysis and statements of compliance.

6. **SECTION 33.28(e).**

a. Rule Text. Section 33.28(e) provides that each EEC must, **"Have all associated software designed and implemented to prevent errors that would result in an unacceptable loss of power or thrust, or other unsafe condition, and have the method used to design and implement the software approved by the Administrator."**

b. Intent of Rule. Section 33.28(e) requires that electrical and electronic engine control systems have all associated software designed and implemented to prevent errors that would result in a unacceptable loss of power or thrust, or other unsafe condition, and have the method used to design and implement the software approved for the application.

c. Background. The following guidance provides a method, but not the only method, of compliance with §33.28(e).

(1) Software Level Requirements. Software designed and implemented according to the standards established as Level 1 or Level A, as provided in RTCA documents DO-178A and DO-178B, respectively, will be viewed as acceptable, provided the applicant has completed

any additional testing required by the Administrator. RTCA Document DO-178A has been superseded by RTCA Document DO-178B. In general, engine certification projects with a date of application after January 11, 1993, should use RTCA Document DO-178B.

(2) Software Partitioning. It may be possible to partition non-critical software from the critical software to allow the non-critical software to be designed and implemented at a lower level than provided in the RTCA documents. Applicants should substantiate the adequacy of the partitioning method and are cautioned to consider whether the partitioned lower software levels are appropriate for any anticipated installations. Should the criticality level requirement be higher in subsequent applications, it would be difficult to raise the software level without repeating the software life cycle processes for the new level.

(3) Software Integrity. RTCA Document DO-178B provides guidance for software used at specified hazard levels. As with all guidance specified in this document, future events or advancements in technology may require modification of that guidance.

APPENDIX A

REGULATORY BASIS FOR REQUIRING ELECTRONIC ENGINE CONTROL (EEC) SYSTEM SAFETY ANALYSIS (SSA) UNDER §33.28

This appendix explains the basis for requiring a System Safety Analysis (SSA) as part of an applicant's demonstration of compliance with §33.28. Prior to §33.28 being added to part 33, EEC systems were certified only upon demonstration of complete redundancy in the electronic portions of critical loops of the system. Applicants that did not perform an SSA were required to demonstrate sufficient similarity to earlier EEC accepted designs that had adequate redundancy. Section 33.28 codified for general applicability the practices used in these early EEC engine certification programs. If changes in EEC design make it no longer possible to accept EECs based on that similarity with earlier accepted designs, then future applicants must, in order to demonstrate compliance with §33.28, submit an SSA for each EEC design.

The FAA will accept new technologies on the basis that the safety and reliability of that new technology are equivalent to, or an improvement over, current technologies. On this basis the EECs were accepted in place of Hydromechanical Engine Control (HMC) designs after establishing the basis for comparison as one loss of thrust control (LOTC) event per 100,000 hours of service. An LOTC event is one in which there is a loss of the ability to control engine thrust from flight idle to 90 percent of maximum rated thrust. This basis for comparison was

established after extensive review, by FAA and industry, of in-service reliability data of existing engine control systems. The results of that review were documented in issue papers and technical memoranda.

To meet this reliability standard, early EEC systems were designed with dual channel redundancy from the sensed inputs to the dual output devices for the critical control loops, defined as the fuel, stator vanes, and bleed control loops. Parts of the engine control system that remained with HMC technology generally were not made redundant.

A means, but not the only means, of compliance with §33.28 is provided in this advisory circular through analysis to demonstrate that the proposed EEC system meets the LOTC criteria and that the EEC system has adequate redundancy and fault accommodation.

Section 33.28 provides that "no single failure or malfunction or probable combination of failures of electrical or electronic components of the control system, results in an unsafe condition." The term "unsafe condition" as used in this context is not limited to those specific conditions described in §33.75. While changes in thrust alone, however, will not always constitute an unsafe condition, the FAA will continue to evaluate unwanted changes in thrust or power with regard to the frequency of those events, their magnitude, and their occurrence in the flight envelope in determining whether a loss of thrust control constitutes an unsafe condition for a particular engine design.New technology electrical and electronic EEC systems introduce

potential failures that could result in unsafe conditions requiring an SSA under §33.28. Those failures include, but are not limited to, the following:

- Complete loss of control over the engine.
- An instability in the control of a critical function of the engine.
- An unwanted change in magnitude or direction of power or thrust in some operating conditions.
- An unwanted action of a critical control function, such as the uncommanded deployment of thrust reversers.

Early EEC system designs have full redundancy on electronic parts of the system that control critical loops and, therefore, were found to provide reliability equivalent to the HMC systems they replaced based on the established reliability criteria of one LOTC event in 100,000 hours of service. These systems are essentially single fault tolerant. They cannot be considered fully single fault tolerant only because a small percentage of failure types either cannot be addressed or are not detectable so that they cannot be accommodated. Using this criteria, subsequent systems can be accepted based on their similarity in design with these early redundant EEC systems. In recent certification programs, however, applicants have proposed engine designs using EEC systems that offer less than full redundancy. In these newer EEC designs significant unwanted changes in thrust or power could occur as a result of single system failures. Therefore, since these newer systems were not similar in design and did not meet the LOTC

reliability criteria equivalent to HMC systems, the FAA could not accept these systems without an SSA to demonstrate compliance with §33.28.

The FAA has recognized that a uniform method for demonstrating how newer EEC systems comply with §33.28 would both promote safety in air commerce and aid industry. This AC provides that method based on meeting the LOTC reliability criteria for HMC designs through tests or analysis, or both. The FAA also recognizes that the LOTC reliability criteria for HMC designs was established through review of service experience data for aircraft certified under part 25 only and that an acceptable reliability criteria for aircraft certified under other standards, parts 23, 27 or 29, may differ from the part 25 criteria. Applicants are cautioned, however, that engines certified under part 33 are generally not restricted to a specific operational use, and that the FAA may, therefore, have to apply the more conservative part 25 criteria in a particular certification program if it determines that the engine involved in that program may be eligible for installation on an aircraft that may be certified under part 25.